STATE OF ALABAMA

Information Technology Guideline

Guideline 660-01G3: Database Security

1. INTRODUCTION:

Malicious attacks against web applications accessing backend databases have increased. One common method of attack, the Structured Query Language (SQL) injection, takes advantage of vulnerable applications and their fully-privileged access to the backend database providing malicious users the means to execute commands in the application's database and gain access to sensitive data.

2. OBJECTIVE:

Improve overall data protection by utilizing native database security mechanisms.

3. SCOPE:

This document provides general guidance that can be applied to any database management system (DBMS); however, this document is not intended to be used to configure database applications such as Microsoft Access that are designed to be used by a single user or a small number of users. Also, this guidance is meant for use in conjunction with the database host platform operating system (OS) baseline as well as other policies, standards, and guidelines related to the requirements of any applications accessing the database.

4. GUIDELINES:

Based on the recommendations of the Defense Information Systems Agency (DISA) found in the Database Security Technical Implementation Guide (STIG), the following guidelines should be used to secure State of Alabama information systems utilizing a DBMS (as described above in Scope).

4.1 SECURITY DESIGN AND CONFIGURATION

4.1.1 Procedural Review

Ensure database security policies and procedures are reviewed at least annually and are current and consistent with current state policy, standards, and guidance, vendor-specific guidance and recommendations, and site-specific or other security policy.

4.1.2 Configuration Specifications

Ensure the database is secured in accordance with the general security requirements specified in state IT policies, standards, and this guideline and with product-specific security guidance in this order of preference as available:

(1) Commercially available practices from independent security organizations such as and the National Institute of Standards and Technology (NIST), DISA, SANS, and the Center for Internet Security (CIS);

(2) Independent testing labs such as ICSA (http://www.icsalabs.com);

(3) Vendor security recommendations and literature.

4.1.3 Compliance Testing

Ensure comprehensive testing plans and procedures for database installations, updates, and patches are defined, documented, and implemented before being deployed in a production environment.

4.1.4 Functional Architecture

As an application, a secure DBMS implementation must be in accordance with a planned or designed usage or architecture. Whenever changes to the usage, environment, or configuration of a DBMS are made or considered, a review of the DBMS functional architecture needs to be completed.

4.1.4.1 Protect external interfaces and information being exchanged

Ensure unused optional database components or features, applications, and objects are removed from the database and host system. If the optional component cannot be uninstalled or removed, then the Database Administrator (DBA) will ensure the unused component or feature is disabled.

Ensure database applications, user accounts, and objects installed for demonstration of database features, experimentation, or other non-production support purposes have been removed from the database and host system.

Configure the database to disable access from the database to objects stored externally to the database on the local host unless mission and/or operationally required and documented in the functional architecture documentation.

Disable use of external procedures by the database unless mission and/or operationally required and documented in the functional architecture documentation.

Ensure database connections to remote databases or remote or external applications and services are disabled and/or not defined unless database replication is in use or the remote connection is mission and/or operationally required and documented in the functional architecture documentation.

Ensure use of credentials used to access remote databases or other applications are restricted to authorized database accounts and used only for mission and/or operationally required and documented purposes.

Ensure credentials stored in or used by the DBMS that are used to access remote databases or other applications are protected by encryption and access controls.

Ensure credentials used to access remote databases or other applications use fully qualified names, i.e., globally unique names that specify all hierarchical classification names, in the connection specification.

Ensure database accounts used for replication or distributed transactions are not granted DBA privileges.

Ensure OS accounts used for execution of external database procedures have the minimum OS privileges required assigned to them.

Ensure each database service or process runs under a custom, dedicated OS account that is assigned the minimum privileges required for operation where applicable.

Ensure database and host system listeners that provide configuration of network restrictions are configured to restrict network connections to the database to authorized network addresses and protocols.

Ensure all local and network-advertised named database services are uniquely and clearly identified.

4.1.4.2 Identify user roles and required access privileges

Ensure all database application user roles and the privileges assigned to them are authorized by the Data Owner in the functional architecture documentation.

4.1.4.3 Identify unique security requirements (encryption of sensitive data)

Ensure security requirements specific to the use of the database are configured as identified in the System Security Plan.

4.1.4.4 Identify categories of sensitive data handled by the database

Ensure all categories of sensitive data stored or processed by the database are identified in the functional architecture documentation.

4.1.4.5 Identify restoration priority of subsystems

Ensure the restoration priority of the database and its supporting subsystems are identified in the System Security Plan.

4.1.5 Non-repudiation

Where encryption, digital signature, key exchange, or secure hashing is used ensure the application of cryptography complies with state encryption standards.

4.1.6 Partitioning the Application

Ensure the DBMS host is dedicated to support of the DBMS and is not shared with other application services including web, application, file, print, or other services unless mission or operationally required and documented in the System Security Plan.

Install and maintain database software directories including DBMS configuration files in dedicated directories or disk partitions separate from the host OS and other applications.

Install and maintain database data directories including transaction log and audit files in dedicated directories or disk partitions separate from software or other application files.

Ensure DBMS data files that store DBMS system tables and other system objects dedicated to support the entire DBMS are not shared with data files used for storage of third-party application database objects.

Ensure database data files used by third-party applications are defined and dedicated for each application.

4.1.7 Ports, Protocols, and Services

Configure DBMS communications to use known and consistent ports, protocols, and services that comply with defined network protection rules.

Ensure random port assignment to network connections is disabled when traversing network firewalls.

4.1.8 Configuration Management (CM) Process

Ensure configuration management procedures are documented and implemented for changes to the DBMS configuration, software libraries, and other related application software libraries.

4.1.9 System Security Plan

Ensure the DBMS is included in or has defined for it a System Security Plan.

Define responsibilities and qualifications for those responsible for administering the security of the database system (this includes specifically the DBA in addition to the standard System Administrator (SA) and Information Security Officer (ISO) roles).

4.1.10 System Library Management Controls

Ensure access to DBMS software is restricted to authorized OS accounts.

Ensure DBMS software is monitored on a regular basis no less frequently than weekly to detect unauthorized modifications.

Ensure database application software is monitored to detect unauthorized modification every week or more often.

Ensure database application software is owned by the authorized application owner account.

Ensure custom application and off-the-shelf source code objects are encoded or encrypted within the production database where supported by the DBMS.

4.1.11 Security Support Structure Partitioning

Ensure the DBMS is not installed on a host system that provides directory services or other security services except when serving as a required component of the security service.

NOTE: This requirement includes the prohibition of a DBMS installation on a Windows Domain Controller.

4.1.12 System State Changes

Ensure all applicable DBMS settings are configured to use trusted files, functions, features, or other components during startup, shutdown, aborts, or other unplanned interruptions.

NOTE: This requirement includes the prevention of scanning for automated job submissions at startup and settings to allow only trusted known good data files at startup.

4.1.13 Software Baseline

Ensure a baseline of database application software and DBMS application objects is maintained for comparison.

NOTE: The baseline of database application software and DBMS application objects requires updating after installation or update.

4.2 IDENTIFICATION AND AUTHENTICATION

4.2.1 Group Identification and Authentication

Group authentication does not provide individual accountability for actions taken on the DBMS or data. Whenever a single database account is used to connect to the database, a secondary authentication method that provides individual accountability is required. Ensure actions by a single database account that is accessed by multiple interactive users are attributable to an individual identifier.

4.2.2 Individual Identification and Authentication

Ensure database user accounts are configured to require individual authentication in order to connect to the DBMS.

Usernames created by default during installation of the DBMS and components are well-known to potential attackers and provide a known target for malicious intent. Change or delete default account usernames.

4.2.2.1 Password Storage

Ensure database account passwords are stored in encrypted format whether stored in database objects, external host files, environment variables or any other storage location.

Encrypt all database account passwords when transmitting across the network.

Do not store database account passwords in batch jobs or application source code.

4.2.2.2 Password Attributes

Assign a database account password at database account creation.

Ensure database passwords differ from previous values by more than 4 characters when changed where supported by the DBMS.

Ensure users are not allowed to change their database account passwords more than once every 24 hours without ISO approval where supported by the DBMS. (This requirement does not apply to password changes after password reset actions initiated by the DBA or application administrator).

Ensure database password complexity standards meet current minimum requirements for length and composition where supported by the DBMS.

Set expiration times for interactive database user account passwords to 60 days or less where supported by the DBMS.

Set expiration times for non-interactive database application account passwords to 365 days or less where supported by the DBMS.

Configure database account passwords to be prevented from reuse for a minimum of five changes or one year where supported by the DBMS.

Configure or test database account passwords to prevent use of easily guessed or discovered values.

Assign custom passwords to all default database accounts whether created by the installation of the database software or database components or by third-party applications.

4.2.3 Key Management

Ensure symmetric keys used for encryption of database user account passwords or other sensitive data used by or for the DBMS are protected and managed in accordance with NSA or NIST-approved key management technology and processes.

Ensure asymmetric keys used for encryption of sensitive data used by or for the DBMS use NSA- or NIST-approved PKI certificates, and ensure the private keys are protected and stored in accordance with NIST-approved key management technology and processes.

4.2.4 Token and Certificate Standards

Where use of username and password is not a sufficiently secure identification and authentication method to restrict access to sensitive data, ensure a NSA- or NIST-approved PKI certificate and an approved hardware security token or an NSA-certified product is used for identification and authentication to the database.

4.3 ENCLAVE AND COMPUTING ENVIRONMENT

4.3.1 Access for Need-to-Know

The least possible access to the fewest possible people provides the least opportunity for misuse of the data.

Ensure all access to sensitive administrative DBMS data stored inside the database and in external host files is granted only to DBA and other authorized administrative database and OS accounts.

Ensure all access to sensitive application data stored inside the database, and in external host files, is granted only to database accounts and OS accounts in accordance with user functions as specified by the Data Owner.

Ensure all access to sensitive application data stored or defined within database objects is granted only to database application user roles and not directly to database application user accounts.

Ensure sensitive application data exported from the database for import to remote databases or applications is not provided to personnel or applications not authorized or approved by the Data Owner.

Ensure production data is not exported for import to development databases except in accordance with processes and procedures approved by the Data Owner.

Ensure database client software includes only database identification parameters of databases to which that user is authorized access.

4.3.2 Audit Record Content

Ensure the DBMS auditing function is enabled.

Ensure all access to DBMS configuration files, database audit data, database credential, or any other DBMS security information is audited.

Ensure all database logons, account locking events, blocking or disabling of a database account or logon source location, or any attempt to circumvent access controls is audited. Where resources are limited, auditing of logons may be reduced to recording only failed logon attempts.

Ensure privileged DBMS actions and changes to security labels or sensitivity markings of data in the DBMS are audited.

Ensure audit records contain the user ID, date and time of the audited event, and the type of the event

Ensure audit records include the reason for any blocking or blacklisting of database accounts or connection source locations.

4.3.3 Audit Trail, Monitoring, Analysis and Reporting

Review database audit data daily.

Employ automated monitoring tools to review DBMS audit data.

Immediately report suspicious or unauthorized activity.

Include the name of the application used to connect to the database in the audit trail where available.

4.3.4 Changes to Data

Configure auditing of access or changes to data in accordance with the application requirements specified in the System Security Plan.

4.3.5 Encryption for Confidentiality - Data at Rest

Ensure applications that access the database are not used with options that display the database account password on the command line.

Ensure sensitive data is encrypted within the database where required by the Data Owner.

Ensure database data files are encrypted where encryption of sensitive data within the DBMS is not available.

4.3.6 Encryption for Confidentiality - Data in Transit

Ensure remote administrative connections to the database are encrypted.

Ensure database communications are encrypted when transmitting sensitive data across untrusted network segments and in accordance with the application requirements.

4.3.7 Data Change Controls

Configure the DBMS to enable transaction rollback and transaction journaling or their technical equivalent to maintain data consistency and recovery during operational cancellations, failures, or other interruptions.

4.3.8 Interconnections among Systems and Enclaves

Ensure interconnections between databases or other applications operating at different classification levels are identified and their communications configured to comply with the interface controls specified in the System Security Plan.

4.3.9 Audit of Security Label Changes

Some DBMS systems provide a feature that assigns security labels to data elements. When this feature is used, enable auditing of any changes to the classification or sensitivity level assigned to sensitive/confidential data in the DBMS (as required by the Data Owner).

4.3.10 Logon

Ensure database connection attempts are limited to a specific number of times within a specific time period as specified in the System Security Plan.

The connection attempts counter may be reset to 0 if the maximum number of failed logon attempts does not occur before the timer is reset. Where this requirement is not compatible with the operation of a front-end application, the unsuccessful logon count and time will be specified and the operational need documented in the System Security Plan.

Configure the DBMS to set the duration of database account lockouts due to unsuccessful logon attempts to an unlimited time that requires the DBA to manually unlock the account.

Configure (where supported by the DBMS) a limit of concurrent connections by a single database account to the limit specified in the System Security Plan, a number determined by testing or review of logs to be appropriate for the application. The limit will not be set to unlimited except where operationally required and documented in the System Security Plan.

4.3.11 Least Privilege

4.3.11.1 Separation of Duties and Least Privilege

> Ensure privileges granted to application user database accounts are restricted to those required to perform the specific application functions.
>
> Ensure database application user roles are restricted to SELECT, INSERT, UPDATE, DELETE, and EXECUTE privileges.
>
> Ensure database application user roles are not granted unauthorized access to external database objects.
>
> Ensure database privileges are assigned via roles and not directly assigned to database accounts. Privileges may be assigned directly to application owner accounts where the DBMS does not otherwise support access via roles.
>
> Ensure database administration OS accounts required for operation and maintenance of the DBMS are assigned the minimum OS privileges required by the specific DBMS to perform DBA functions.

Ensure database application objects are owned by an authorized application object owner account.

Ensure the minimum database administrative privileges are assigned to database administrative roles to perform the administrative job function.

Review monthly or more frequently the database privileges assigned to database administrative roles to ensure they are limited to the minimum required.

Restrict restore permissions on databases to DBAs and/or the database owners.

Ensure developers are not granted system privileges within a production database.

4.3.11.2 Privileged accounts accessible only by privileged users

Restrict access to the DBMS software installation account to ISO-authorized personnel only.

Ensure use of the DBMS software installation account is logged and/or audited to indicate the identity of the person who accessed the account.

Restrict database privileged role assignments to ISO-authorized accounts.

Ensure privileged database accounts are used only for privileged database job functions, and ensure non-privileged database accounts are used to perform non-privileged job functions.

4.3.11.3 Use privileged accounts only for privileged functions

Ensure custom application owner accounts are disabled or locked when not in use.

Ensure the DBMS software installation account is only used when performing software installation and upgrades or other DBMS maintenance. The ISO will ensure the DBMS software installation account is not used for DBA activities not related to DBMS file permission and ownership maintenance.

Monitor database batch and job queues to ensure no unauthorized jobs are accessing the database.

4.3.12 Marking and Labeling

Configure DBMS marking and labeling of non-public data where required in accordance with the System Security Plan.

4.3.13 Conformance Monitoring and Testing

Ensure the DBMS is included in the periodic testing of conformance with vulnerability management and configuration requirements.

4.3.14 Privileged Account Control

Ensure all database administrative privileges defined within the DBMS and externally to the database are assigned using DBMS or OS roles.

Review DBA role assignments whenever changes to the assignments occur.

4.3.15 Production Code Change Controls

Ensure application developer database accounts are assigned limited privileges in order to protect production application objects.

Review, at least every three months, privileges granted to developers on shared production/development database systems that allow modification of application code or application objects.

Ensure developer accounts on a shared production/development host system are not granted operating system privileges to production files, directories, or database components.

4.3.16 Resource Control

Ensure DBMS resource controls are enabled to clear residual data from released object stores.

4.3.17 Audit Reduction and Report Generation

Requirements stated in State IT Standard 670-06S1: Log Management.

4.3.18 Audit Record Retention

Requirements stated in State IT Standard 670-06S1: Log Management.

4.3.19 Security Configuration Compliance

Ensure the DBMS host and related applications and components comply with all applicable policies, standards, and baselines.

4.3.20 Software Development Change Controls

Ensure database applications do not use DDL statements except where dynamic object structures are required. The statements used to define objects in the database are referred to as DDL statements and include CREATE, DROP, and ALTER object statements. (DDL statements do not include CREATE USER, DROP USER, or ALTER USER actions.)

Ensure software development on a production system is separated through the use of separate and uniquely identified data and application file storage partitions and processes/services.

4.3.21 Audit Trail Backup

Ensure the DBMS audit logs are included in DBMS backup procedures.

4.3.22 Audit Trail Protection

Ensure DBMS audit records are protected from unauthorized access.

4.3.23 Account Control

Ensure unauthorized database accounts are removed or disabled.

Monitor database account expiration and inactivity and remove expired accounts and accounts that are inactive for 60 days or longer.

4.4 ENCLAVE BOUNDARY DEFENSE

4.4.1 Boundary Defense

Ensure the DBMS is protected from direct client connections from public or unauthorized networks.

4.4.2 Remote Access for Privileged Functions

Ensure remote administration of the database is not enabled or configured unless mission and/or operationally required and authorized by the ISO.

Configure auditing of all actions taken by database administrators during remote sessions.

Review daily audit trails of remote administrative sessions to discover any unauthorized access or actions. Weekly review is required by State IT Standard 640-02S4: Remote Maintenance.

Restrict remote administration connections to the database to dedicated and encrypted network addresses and ports.

4.5 CONTINUITY

4.5.1 Protection of Backup and Restoration Assets

Ensure files critical to database recovery are protected by employment of database and OS high-availability options such as storage on RAID devices.

Ensure access to database backup and recovery files are restricted to the database and/or OS backup and recovery processes, DBAs, and database backup/recovery operators.

4.5.2 Data Backup Procedures

Backup database data, configuration, and other files critical to database operation at intervals consistent with the database's assigned criticality level.

4.5.3 Disaster and Recovery Planning

Document, implement, and test the DBMS backup and recovery strategy at least semi-annually.

4.5.4 Backup Copies of Critical Software

Ensure critical database software directories are backed up.

4.5.5 Trusted Recovery

Configure the DBMS to use only authorized software, data files, or other critical files during recovery.

4.6 VULNERABILITY MANAGEMENT

Remove or upgrade unsupported DBMS software prior to a vendor dropping support.

Create a formal migration plan for removing or upgrading DBMS systems 6 months prior to the date the vendor drops security patch support.

Ensure all applicable vendor-provided security patches are installed in accordance with State policy/standards.

5. ADDITIONAL INFORMATION:

5.1 POLICY

Information Technology Policy 660-01: Application Security
http://isd.alabama.gov/policy/Policy_660-01_Application_Security.pdf

5.2 RELATED DOCUMENTS

Information Technology Dictionary
http://isd.alabama.gov/policy/IT_Dictionary.pdf

Information Technology Standard 670-03S1: Vulnerability Management
http://isd.alabama.gov/policy/Standard_670-03S1_Vulnerability_Management.pdf

Information Technology Standard 670-06S1: Log Management
http://isd.alabama.gov/policy/Standard_670-06S1_Log_Management.pdf

DISA Database STIG
http://iase.disa.mil/stigs/stig/index.html

Signed by Art Bess, Assistant Director

6. DOCUMENT HISTORY

Version	Release Date	Comments
Original	7/14/2008	